

REMARKS

STATUS OF CLAIMS

Note that Claims 3, 5-8, 12-15, 17, 21-23, 26-27, and 34 were previously cancelled.

Claims 1, 2, 10, 18, 24, 25, 28, 29, 32, 33, 35-37, 39, 42, 45-47, 49, and 52 have been amended.

No claims have been cancelled, added, or withdrawn herein.

Claims 1-2, 4, 9-11, 16, 18-20, 24-25, 28-33, and 35-54 are currently pending in the application.

SUMMARY OF THE REJECTIONS/OBJECTIONS

Claims 1, 2, 18, 24, 25, 32, 33, 35, 36, 42, 45, 46, and 52 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite. Claims 1, 2, 4, 9-11, 16, 18-20, 24, 25, 28, 29, 32, 33, and 35-54 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent Number 6,957,346 issued to Kivinen et al. (" *Kivinen* ") in view of U.S. Patent Application Publication Number 2002/0046348 of Brustoloni (" *Brustoloni* "). The rejections are respectfully traversed.

The Applicant notes that Claims 30 and 31 have been allowed in the Final Office Action.

ADMINISTRATIVE MATTERS RE: STATUS OF DRAWINGS AND SOME CLAIMS

As a preliminary matter, neither the recently issued Final Office Action or the previously issued first Office Action indicate the status of the drawings as originally filed with the Application on January 17, 2002 in the Office Action Summaries under the heading "Application Papers," item 10. Therefore, the Applicant respectfully requests that the status of the drawings (e.g., whether accepted or objected to) be indicated in the next communication from the Office.

As another preliminary administrative matter, the following claims are not listed in item 7 on page 3 of the Final Office Action as being rejected under 103(a) over *Brustoloni* in view of *Kivinen*, nor are these claims addressed in the Detailed Action in which the relevant portions of the prior art are applied to the claims, yet all of these claims are listed on the

Office Action Summary, item 6 under “Disposition of Claims, as being rejected: Claims 2, 11, 16, 36, 40, 45, and 46. Thus, while it appears that the Final Office Action has rejected Claims 2, 11, 16, 36, 40, 45, and 46 over *Brustoloni* in view of *Kivinen*, there is no indication within the Final Office Action as to the basis of these rejections based upon those prior art references. Therefore, the Applicant respectfully requests that Claims 2, 11, 16, 36, 40, 45, and 46 be addressed in the next communication from the Office.

However, for the purposes of this response, the Applicant is proceeding on the basis that Claims 2, 16, 36, 40, 45, and 46 are rejected over *Brustoloni* in view of *Kivinen*. Since Claim 45 is an apparatus claim that includes many of the same features as in method Claim 1, computer-readable medium Claim 32, and apparatus Claim 35, the Applicant will proceed on the basis that Claim 45 is rejected similarly as with Claims 1, 32, and 35. Also, the Applicant will proceed on the basis that Claims 2, 36, and 46 are rejected similarly to Claims 1, 35, and 45 that are the corresponding independent claims and that included similar features. Also, because Claim 16 includes similar features as with Claims 41 and 51, the Applicant will proceed on the basis that Claim 16 is rejected similarly to Claims 41 and 51. Finally, because Claims 11 and 40 have similar features as with Claim 50, the Applicant will proceed on the basis that Claims 11 and 40 are rejected similarly as with Claim 50.

EXPLANATION OF AND SUPPORT FOR CLAIM AMENDMENTS

Claims 1, 2, 10, 18, 24, 25, 28, 29, 32, 33, 35-37, 39, 42, 45-47, 49, and 52 have been amended and are fully supported by the originally filed disclosure. No new matter is included.

Specifically, Claims 1, 24, 25, 32, 33, 35, and 45 have been amended to feature that “the first identifier is a first IPsec Security Parameter Index (SPI),” and “the second identifier is a second IPsec SPI.” Similarly, Claims 2, 18, 36, 42, 46, and 52 are amended to feature that “the third identifier is a third IPsec SPI.” Also, Claims 10, 28, 29, 39, and 49 have been amended to remove features that are now duplicative with respect to the corresponding independent claims (e.g., that the identifiers are IPsec SPIs), and Claims 10, 39, and 49 included other changes to ensure consistent use of these terms. These amendments are supported by originally filed Claim 10 that featured that the first and second identifiers were first and second IPsec SPIs as well as by the Application by at least the disclosures of

paragraphs [0026, 0041, 0060, 0064, 0068, 0072, 0076] that explain that the identifiers can be IPsec SPIs.

Claims 1, 32, 35, and 45 have also been amended to feature that “the specified scheme is a computer-implemented operation that is known to both the device that employs address translation and a second node.” Similarly, Claims 24, 25, and 33 have also been amended to feature that “the specified scheme is a computer-implemented operation that is known to both the device that employs address translation and the first node.” These amendments are included as requested in the Final Office Action and are supported by the Application, as discussed below in the following section regarding the rejections under 35 U.S.C. § 112, second paragraph.

Finally, Claims 37 and 47 are amended to correct typographical errors so that each of these claims correctly refers to the “Message Digest 5 on-way hash function,” which is described in the Application in paragraph [0044] instead of other numerals that were inadvertently included in the previous response.

RESPONSE TO REJECTIONS NOT BASED ON THE PRIOR ART

Claims 1, 2, 18, 24, 25, 32, 33, 35, 36, 42, 45, 46, and 52 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite. Specifically, the Final Office Action states: “The term ‘a specified scheme’ in claims 1, 2, 24, 35-36 and 45-46...renders the claim[s] indefinite. The term a specified scheme is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the claim. Applicant is advised to define ‘specified scheme’ in the claims to particularly point out and distinctly claim the subject matter which applicant regards as the invention.”

The Applicant respectfully disagrees that the term “a specified scheme” is unclear as the term “a specified scheme” is the subject of the subsections of the Application titled “A. Approaches for Generating Result Values Based on Initial Identifiers” and “B. Generating a Subsequent Identifier Based on a Result Value,” which encompasses paragraphs [0060-0067].

In particular, the first of these two subsections of the Application explains that a specified scheme is “used to generate a result value based on a particular input value.”

(Paragraph [0061].) The Application provides several examples of “a specified scheme,” such as the Message Digest 5 (MD5) hash function, the use of other hash functions, adding the value “1” to the input value to produce the result value, or to reverse the bytes of the input value to produce the result value. (Paragraph [0061].) In addition, the second of these two subsections of the Application explains that “any approach may be used to generate the subsequent identifier based on the specified scheme that uses the initial identifier **as long as the selected approach is known to both the node from which a response message is sent based on an initial message and the device employing address translation.**” (Paragraph [0065].)

However, to address the rejection and expedite the examination of the present application, the Applicant has amended Claims 1, 24, 25, 32, 33, 35, 45, in which the term “a specified scheme” is first introduced to feature “wherein the specified scheme is a computer-implemented operation that is known to both the device that employs address translation and a second node.”

Therefore, the Applicant respectfully submits that the amendments described above that define the term “a specified scheme” and that related that definition to the other features of the corresponding claims traverse the rejection under 35 U.S.C. § 112, second paragraph, of Claims 1, 2, 18, 24, 25, 32, 33, 35, 36, 42, 45, 46, and 52.

RESPONSE TO REJECTIONS BASED ON THE PRIOR ART

A. CLAIM 1

(1) INTRODUCTION TO CLAIM 1

Claim 1 features:

“A method for facilitating Internet security protocol (IPsec) based communications through a device that employs address translation in a telecommunications network, the method comprising the steps of:

receiving a first electronic message from a first node, wherein:

the first node is associated with a first network address;

the first electronic message is based on IPsec;

the first electronic message is associated with a first identifier;

the first identifier is a **first IPsec Security Parameter Index (SPI)**;
the first identifier is generated by the first node; and
the first electronic message is addressed to a second network address;
the device generating a value based on the first identifier and a specified scheme,
wherein the specified scheme is a computer-implemented operation that is
known to both the device that employs address translation and a second node;
sending the first electronic message to [[a]] the second node based on the second
network address, wherein the first electronic message includes a particular
network address that is associated with the device instead of the first network
address;
receiving a second electronic message from the second node, wherein:
the second electronic message is based on IPsec;
the second electronic message is addressed to the particular network address;
the second electronic message is associated with a second identifier that is
different than the first identifier; ~~and~~
the second identifier is a **second IPsec SPI**; and
the second identifier is generated, based on the first identifier and the
specified scheme, by the second node;
the device determining whether the second electronic message is directed to the first
node based on the value and the second identifier; and
sending the second electronic message to the first node at the first network address
when the second electronic message is determined to be directed to the first
node.” (Emphasis added.)

Thus, Claim 1 as amended herein features the use of IPsec security parameter indexes (SPIs) as the identifiers, that the second identifier/IPsec SPI is generated based on the first identifier/IPsec SPI, and that the NAT enabled device determines that the second electronic message is directed to the first node based on the second identifier/IPsec SPI that is generated based on the first identifier/IPsec SPI. As a result of this amendment, Claim 1 now includes features that are similar to Claims 30 and 31, which the Final Office Action indicates are directed to allowable subject matter based on these similar features.

(2) INTRODUCTORY DISCUSSION OF *BRUSTOLINI* AND *KIVINEN*

In contrast to the approach of Claim 1, *Brustoloni* discloses an approach for interoperation of NAT with IKE and ESP tunnel mode of IPsec. (*Brustoloni*, Abstract.) In particular, *Brustoloni* uses “pings,” or control packets, over a tunnel and waiting to send normal data packets until a response to the ping is received from the pinged server. (*Brustoloni*, Abstract.) Thus, by using the pings and waiting for responses thereto, *Brustoloni* is able to accommodate IPsec with NAT. However, this is fundamentally different than the approach of Claim 1 in which the SPI for one node is based on the SPI for another node, and *Brustoloni* fails to disclose anything related to such a feature.

Also in contrast to the approach of Claim 1, *Kivinen* also discloses an approach for using IPsec with NAT. (*Kivinen*, Abstract.) In particular, *Kivinen* determines transformations that occur on a packet and then compensate for those transformations, with encapsulation of IPsec AH/ESP packets into UDP packets for transport. (*Kivinen*, Abstract.) . However, this is fundamentally different than the approach of Claim 1 in which the SPI for one node is based on the SPI for another node, and *Kivinen* fails to disclose anything related to such a feature.

(3) THE FINAL OFFICE ACTION’S CITATIONS FROM *BRUSTOLINI* AND *KIVINEN*

The Final Office Action states that *Kivinen* discloses “receiving a first electronic message from a first node, wherein the first electronic message is based on IPsec and is associated with a first identifier (col 3 lines 7-14 and col 7 lines 51-60); the first identifier is generated by the first node (col 7 lines 51-60)...” However, the first cited portion of *Kivinen* merely describes that the reference describes securely communicating packets between two devices through an intermediate device that performs NAT, which discloses nothing about a node generating an identifier, little less an IPsec SPI. (*Kivinen*, Col. 3, lines 7-14.) Furthermore, in the second cited portion of *Kivinen*, which describes Phase 1 of IKE between an Initiator and a Responder, the only thing that appears to match the “identifier” of Claim 1 is the “certain Vendor ID Payload.” (*Kivinen*, Col. 7, lines 51-60.) However, contrary to the assertion of the Final Office Action, there is nothing in this or any other portion of *Kivinen* that discloses that this “certain Vendor ID Payload” is generated by the either the Initiator or the Responder, and the name “certain Vendor ID Payload” indicates that this is data is used to

identify one vendor from another, and thus would not be generated by either the Initiator or the Responder. In addition, as amended above, Claim 1 now features that “the first identifier is a **first IPsec Security Parameter Index (SPI)**,” and there is nothing within Kivinen discloses that the “certain Vendor ID Payload” is an IPsec SPI.

The Final Office Action also states that *Kivinen* discloses “the device determining whether the second electronic message is directed to the first node based on the value and the second identifier; and sending the second electronic message to the first node at the first network address when the second electronic message is determined to be directed to the first node (col 3 lines 15-28 and col 7 line 60 through col 8 line 7).” However, the first cited portion describes the overall method of *Kivinen*, namely of determining what network address translations occur, if any, then encapsulating packets that conform to a first protocol into packets conforming to a second protocol, transmitting those encapsulated packets, and decapsulating the packets (*Kivinen*, Col. 3, lines 15-28), none of which discloses anything about a “second identifier” as in Claim 1 that is a second IPsec SPI that is generated, based on the first identifier/IPsec SPI.

The second cited portion of *Kivinen* describes Figure 3, and in particular, the Vendor IP fields in the Initiator’s first Phase 1 message (e.g., 201’) and the Responder’s first Phase 1 message (e.g., 201”), explaining that the “Vendor ID” field in the Vendor ID Payload is “basically an identification of that method,” namely the method that is being supported. (*Kivinen*, Col. 7, lines 61-67.) *Kivinen* then explains that this “Vendor ID” is the MD5 hash of a previously known identification string, such as “SSH DSEC NAT Traversal Version 1,” which is the “method” referred to at the bottom of Column 7. (*Kivinen*, Col. 8, lines 1-7.) Note that this means the Vendor ID is fixed or the same for both the Initiator and Responder, thus are not different as in Claim 1, nor that the Vendor ID is an IPsec SPI as are the identifiers in Claim 1 as amended above, and little less that the second IPsec SPI is generated based on the first IPsec SPI, as in Claim 1.

The Final Office Action correctly states that *Kivinen* does not teach that “the second electronic message is associated with a second identifier that is different than the first identifier and that the second identifier is generated based on the first identifier and the specific scheme by the second node.” Then the Final Office Action states that *Brustolini* discloses these features of Claim 1, citing paragraphs [0013, 0029, 0044] and Figure 2.

However, paragraph [0013] of *Brustoloni* explains that the “VPN Masquerade” maintains a hash table of client and server IP addresses and initiator and responder cookies, that when a client sends a packet that doesn’t match an item in the table, an item is created, and that when a server sends packets such that no established item in the table matches but an outstanding item does match, that the that item is converted into an established item. (*Brustoloni*, Paragraph [0013].) However, this says nothing about a second identifier being generated by a second node based on a first identifier generated by a first node, in which the second identifier is generated on the first, and that both identifiers are IPsec SPIs, as in Claim 1.

Next, paragraph [0029] of *Brustoloni* describes that transmission of actual data packets are delayed until an item is established by the NAT device, which is achieved by enforcing a requirement that the client wait until the item is established before trying to establish a new one via the use of the “ping” control packets. (*Brustoloni*, Paragraph [0029].) As a result, if two clients randomly select the same incoming SPI, at least one of the clients will not receive a response to its “ping, thereby causing that client to rekey its tunnel and choose a different incoming SPI, thereby avoiding a collision. (*Brustoloni*, Paragraph [0029].)

Note that while this approach appears to address a similar problem to that being addressed by the Applicant’s application, the solution is quite different, namely that *Brustoloni* blocks the second client from negotiating the IPsec SA until the first client has successfully performed its negotiation of its own SA. In contrast, the approach of Claim 1 avoids the “collision” problem of two clients communicating with the same responding server by having the responding server generate it’s SPI based on the corresponding SPI of the originating server, thereby allowing the NAT device to determine to which client a particular response is to go to by matching part of the responding server’s SPI to the client SPI. However, there is nothing in this or any other portion of *Brustoloni* that describes that the responding server generates its SPI based on the client SPIs, as in the approach of Claim 1.

Finally, the Final Office Action states that “it would have been obvious to one having ordinary skill in the art at that time the invention was made to employ the teaching method of *Brustoloni* with *Kivinen* because it would secure the method by routing the incoming packets from a common server to a plurality of clients that are communicating with the server and sharing a common access link (*Brustoloni* See 0028).” However, it is unclear to the Applicant how the teachings of *Kivinen*, which encapsulates the IPsec traffic that normally cannot be

accommodated by a NAT device by using another protocol such as UDP, thereby effectively “hiding” that the traffic is based on IPsec from the NAT device, with the teachings of *Brustoloni* that performs no such encapsulation of the IPsec traffic and rather must see the IPsec traffic in order to enforce *Brustoloni*’s “ping” approach by preventing another client from “pinging” the same server until the first client establishes its own SA with the server.

Furthermore, *Kivinen* is being relied upon as disclosing the “first identifier” of Claim 1, which is being matched by the Final Office Action to the “Vendor ID,” whereas *Brustoloni* is being relied upon as disclosing the “second identifier” of Claim 1, which is generated based on “the first identifier,” which means the “Vendor ID” of *Kivinen*. Yet there is nothing in *Brustoloni* about a “Vendor ID” as disclosed in *Kivinen*, little less that *Brustoloni* generates another identifier based on such a “Vendor ID.”

Finally, the Applicant has reviewed the remaining portions of both *Kivinen* and *Brustoloni* for anything about the generation of a “second identifier/IPsec SPI” based on a “first identifier/IPsec SPI,” as in Claim 1. While both references deal with IPsec and thus refer to the SPIs that are generated according to IPsec, the Applicant has been unable to locate anywhere within either *Kivinen* or *Brustoloni* any disclosure that one IPsec SPI is generated based on another IPsec SPI, as in Claim 1.

(4) CONCLUSION OF DISCUSSION OF CLAIM 1 AND *BRUSTOLINI* AND *KIVINEN*

Because *Brustolini* and *Kivinen*, either alone or in combination, fail to disclose, teach, suggest, or in any way render obvious “receiving a first electronic message from a first node, wherein:... the first electronic message is based on IPsec; the first electronic message is associated with a first identifier; the first identifier is a first IPsec Security Parameter Index (SPI); the first identifier is generated by the first node;... receiving a second electronic message from the second node, wherein: the second electronic message is based on IPsec;... the second electronic message is associated with a second identifier that is different than the first identifier; the second identifier is a second IPsec SPI; and the second identifier is generated, based on the first identifier and the specified scheme, by the second node;” the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

C. CLAIMS 24-25, 32, 33, 35, AND 45

Claims 24-25, 32, 33, 35, and 45 contain features that are either the same as or similar to those described above with respect to Claim 1. For example, Claims 32, 35, and 45 all feature “receiving a first electronic message from a first node, wherein:... the first electronic message is based on IPsec; the first electronic message is associated with a first identifier; the first identifier is a first IPsec Security Parameter Index (SPI); the first identifier is generated by the first node;... receiving a second electronic message from the second node, wherein: the second electronic message is based on IPsec;... the second electronic message is associated with a second identifier that is different than the first identifier; the second identifier is a second IPsec SPI; and the second identifier is generated, based on the first identifier and the specified scheme, by the second node;” which is the same as in Claim 1.

As another example, Claims 24 and 33 both feature “receiving a first electronic message from a first node, wherein:... the first electronic message is based on IPsec; the first electronic message is associated with a first identifier; the first identifier is a first IPsec Security Parameter Index (SPI); the first identifier is generated by the first node based on a second identifier and a specified scheme;... receiving a second electronic message from the second node, wherein: the second electronic message is based on IPsec;... the second electronic message is associated with a second identifier;...the second identifier is generated by the second node;” which is similar to Claim 1.

And as a final example, Claim 25 features “generating a value based on both a first identifier that is associated with a first node and a specified scheme, wherein: the first identifier is generated by the first node; the first identifier is a first IPsec Security Parameter Index (SPI);...wherein the second identifier is a second IPsec SPI;... receiving...a first electronic message that originates from the first node, wherein: the first electronic message is based on IPsec; the first electronic message is associated with the first identifier;...generating a second electronic message, wherein: the second electronic message is based on IPsec; the second electronic message is associated with the second identifier;” which is similar to Claim 1.

Therefore, based on at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claims 24-25, 32, 33, 35, and 45 are allowable over the art of record and are in condition for allowance.

D. CLAIMS 2, 4, 9-11, 16, 18-20, 28-29, 36-44, AND 46-54

Claims 2, 4, 9-11, 16, and 18-20 are dependent upon Claim 1, Claims 28-29 are dependent upon Claim 25, Claims 36-44 are dependent upon Claim 35, and Claims 46-54 are dependent upon Claim 45. Each of Claims 2, 4, 9-11, 16, 18-20, 28-29, 36-44, and 46-54 is therefore allowable for the reasons given above for Claims 1, 25, 35, and 45. In addition, each of Claims 2, 4, 9-11, 16, 18-20, 28-29, 36-44, and 46-54 introduces one or more additional limitations that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those limitations is not included at this time. Therefore, it is respectfully submitted that Claims 2, 4, 9-11, 16, 18-20, 28-29, 36-44, and 46-54 are allowable for the reasons given above with respect to Claims 1, 25, 35, and 45.

APPLICANT COMMENTS ON “ALLOWABLE SUBJECT MATTER”

The Final Office Action acknowledges that Claims 30 and 31 are directed to allowable subject matter, and then the Final Office Action provides reasons for why Claims 30 and 31 are allowable over the prior art. However, among the reasons given for why Claims 30 and 31 are allowable is the following: “the NAT device can make an entry in the network address translation table that properly associates the correct originator node to the responder node for each security association established between original nodes and the same responder node.”

While this quoted portion from the Final Office Action correctly explains the application of the approach of Claims 30 and 31 to an implementation that includes a network address translation table that stores data on the security associations between IPsec originator and IPsec responder nodes, none of the features in this quoted portion of that discussion from the Final Office Action are included in either of Claim 30 and 31. Therefore, the Applicant wishes to make the record clear that Claims 30 and 31 do not include these features from the quoted portion of the Final Office Action and that Claims 30 and 31 are not limited to implementations that include those features from the quoted portion of the Final Office Action.

CONCLUSION

The Final Office Action acknowledges that Claims 30-31 are directed to allowable subject matter.

The Applicant believes that all issues raised in the Final Office Action have been addressed and that allowance of the pending claims is appropriate. After entry of the amendments, further examination on the merits is respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

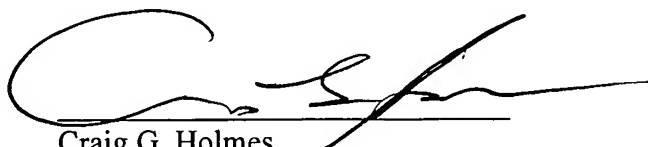
For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP



Craig G. Holmes
Reg. No. 44,770

Date: July 17, 2006

2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
Telephone: (408) 414-1207
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, Mail Stop RCE, P.O. Box 1450, Alexandria, VA 22313-1450.

on July 17, 2006 by Susan Jensen
Susan Jensen